

# United States District Court

for the  
Western District of New York

In the Matter of the Search of

*(Briefly describe the property to be searched or identify the person by name and address.)*

37 Lehigh Street, Buffalo, New York 14206

Case No. 19-mj-1042

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

**37 Lehigh Street, Buffalo, New York 14206, which is more fully described and pictured in Attachment A, which is attached hereto and incorporated by reference herein.**

located in the Western District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

**Evidence pertaining to violations of Title 18, U.S.C. §§ 2251(a), 2252A(a)(2) and 2252A(a)(5)(B), as more fully set forth in Attachment B, which is attached hereto and incorporated by reference herein.**

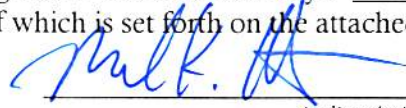
The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of Title 18 U.S.C. Sections 2251(a), 2252A(a)(2) and 2252A(a)(5)(B).

The application is based on these facts:

- ☒ continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

MICHAEL HOCKWATER  
TASK FORCE OFFICER  
FEDERAL BUREAU OF INVESTIGATION  
Printed name and title

Sworn to before me and signed in my presence.

Date: April 15, 2019

City and state: Buffalo, New York

  
Judge's signature  
HONORABLE JEREMIAH J. MCCARTHY  
UNITED STATES MAGISTRATE JUDGE  
Printed name and Title

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Michael Hockwater, being duly sworn, depose and say:

1. I am a Police Detective with the Town of Cheektowaga, New York Police Department. I have been a Police Officer since August of 1989. I am currently assigned as a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI), Buffalo Field Office, Child Exploitation Task Force, Innocent Images National Initiative, which targets individuals involved in the online sexual exploitation of children. I have been a TFO since June 14, 2010. As part of these duties, I have become involved in the investigation of suspected violations of Title 18, United States Code, Sections 2251, 2252, 2252A, 2422, and 2423. I have also participated in various FBI mandated and volunteer training for the investigation and enforcement of federal child pornography laws in which computers and electronic media are used as the means for receiving, transmitting, and storing child pornography.

2. I make this affidavit in support of an application for a warrant to search the residence known as **37 Lehigh Street, Buffalo, New York 14206** (hereinafter the "SUBJECT PREMISES"), located in the Western District of New York, which is more fully described and pictured in **Attachment A**.

3. The statements contained in this affidavit are based on my involvement in this investigation, as well as information provided to me by other law enforcement officers involved in this investigation, and upon my training and experience. Because this affidavit is being submitted for the limited purpose of seeking a search warrant, I have not included

each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18 U.S.C. Section 2251(a) [production of child pornography], Title 18 U.S.C. Section 2252A(a)(2) [receipt of child pornography] and 18 U.S.C. Section 2252A(a)(5)(B) [possession of child pornography] exists at the SUBJECT PREMISES.

### **I. COMPUTERS AND CHILD PORNOGRAPHY**

4. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these images on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.

5. The development of computers has significantly reduced the amount of resources needed to produce, communicate, distribute, and share child pornography.

6. Child pornographers can now transfer photographs from a camera into a computer readable format with a device known as a scanner. With the advent of digital cameras, the images can now be captured on a digital camera and transferred directly onto a

computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 4 gigabytes of data, which provides enough space to store over 1000 high resolution photographs. Video camcorders, which once recorded video onto tapes or mini CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer. A device known as a modem allows any computer to connect to another computer through the use of a telephone, cable, or wireless connection. Additionally, it is now commonplace for cellular telephones to be equipped with photo and video capabilities, which allows an individual to digitally shoot, store, send, and/or receive child pornography all with one device. Additionally, cellular telephones can be used as a means of communications through the use of text and electronic mail ("e-mail") messages. Electronic contact can be made to literally millions of computers around the world.

7. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously

within the last several years. These drives can store hundreds of thousands of images at very high resolution.

8. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

9. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

10. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and attempt to receive child pornography:

- a. Those who receive and attempt to receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

- b. Those who receive and attempt to receive child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Those who receive and attempt to receive child pornography often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d. Likewise, those who receive and attempt to receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.
- e. Those who receive and attempt to receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- f. Those who receive and attempt to receive child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

11. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this

information can be intentional, i.e., by saving an e mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Additionally, a computer also creates logs, indices, and registries indicating when a computer was used, which user was logged on, and when data was accessed, shared, transferred, or downloaded. A forensic examiner can often recover evidence which shows that a computer contains peer to peer software (see below), when the computer was sharing files, and even some of the files which were uploaded or downloaded. Such information may be maintained indefinitely until overwritten by other data. Cellular telephones also allow the user to save or store text messages and e mail messages received by the phone, for later viewing or distributing, and even if deleted, a forensic examiner can often recover evidence of such text messages and e mail messages.

12. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider (ISP) that connects to the Internet. The ISP assigns each user an Internet Protocol (IP) Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number

is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing, that is, they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses may also be static, if an ISP assigns a user's computer a particular IP address that is used each time that computer accesses the Internet. The ISP may log the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

13. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files,



and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

14. Digital computer files can be analyzed using a variety of different computer algorithms, which reads a particular computer file and generates a unique numeric identifier for the file, known as a "hash value." By comparing these hashes it can be concluded that two files that share the same digital signature are identical with a precision that exceeds 99.99 percent certainty. Even the slightest modification of a file will change its hash value. Your Affiant is unaware of a documented occurrence of two different files having different contents while sharing the same hash value.

### **Instagram**

15. From my review of publicly available information provided by Instagram about its service, including Instagram's "Privacy Policy," I am aware of the following about Instagram and about the information collected and retained by Instagram.

16. Instagram is operated by Facebook Inc. Instagram can be accessed at <http://www.instagram.com>. Instagram allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and other information. Users can access Instagram through the Instagram website or by using a special electronic

application (“app”) created by the company that allows users to access the service through a mobile device.

17. Instagram permits users to post photos to their profiles on Instagram and otherwise share photos with others on Instagram, as well as Facebook and Twitter. When posting or sharing a photo on Instagram, a user can add to the photo: a caption; various “tags” that can be used to search for the photo (e.g., a user may add the tag #vw so that people interested in Volkswagen vehicles can search for and find the photo); location information; and other information. A user can also apply a variety of “filters” or other visual effects that modify the look of the posted photos. In addition, Instagram allows users to make comments on posted photos, including photos that the user posts or photos posted by other users of Instagram. Users can also “like” photos.

18. Upon creating an Instagram account, an Instagram user must create a unique Instagram username and an account password. This information is collected and maintained by Instagram.

19. Instagram asks users to provide basic identity and contact information upon registration and also allows users to provide additional identity information for their user profile. This information may include the user’s full name, e-mail addresses, and phone numbers, as well as potentially other personal information provided directly by the user to Instagram. Once an account is created, users may also adjust various privacy and account settings for the account on Instagram. Instagram collects and maintains this information.

20. Instagram allows users to have “friends,” which are other individuals with whom the user can share information without making the information public. Friends on Instagram may come from either contact lists maintained by the user, other third-party social media websites and information, or searches conducted by the user on Instagram profiles. Instagram collects and maintains this information.

21. Instagram also allows users to “follow” another user, which means that they receive updates about posts made by the other user. Users may also “unfollow” users, that is, stop following them or block them, which prevents the blocked user from following that user.

22. Instagram allow users to post and share various types of user content, including photos, videos, captions, comments, and other materials. Instagram collects and maintains user content that users post to Instagram or share through Instagram.

23. Instagram users may send photos and videos to select individuals or groups via Instagram Direct. Information sent via Instagram Direct does not appear in a user's feed, search history, or profile.

24. Users on Instagram may also search Instagram for other users or particular types of photos or other content.

25. For each user, Instagram also collects and retains information, called “log file” information, every time a user requests access to Instagram, whether through a web page or

through an app. Among the log file information that Instagram's servers automatically record is the particular web requests, any Internet Protocol ("IP) address associated with the request, type of browser used, any referring/exit web pages and associated URLs, pages viewed, dates and times of access, and other information.

26. Instagram also collects and maintains "cookies," which are small text files containing a string of numbers that are placed on a user's computer or mobile device and that allows Instagram to collect information about how a user uses Instagram. For example, Instagram uses cookies to help users navigate between pages efficiently, to remember preferences, and to ensure advertisements are relevant to a user's interests.

27. Instagram also collects information on the particular devices used to access Instagram. In particular, Instagram may record "device identifiers," which includes data files and other information that may identify the particular electronic device that was used to access Instagram.

28. Instagram also collects other data associated with user content. For example, Instagram collects any "hashtags" associated with user content (i.e., keywords used), "geotags" that mark the location of a photo and which may include latitude and longitude information, comments on photos, and other information.

29. Instagram also may communicate with the user, by email or otherwise. Instagram collects and maintains copies of communications between Instagram and the user.

## **II. THE INVESTIGATION AND PROBABLE CAUSE**

30. On April 10, 2019, I was contacted by Detective Dawn Rosenberry of the Fauquier County Sheriff's Office in the state of Virginia who requested assistance with an investigation involving the production of child pornography. Detective Rosenberry opened an investigation in response to a report she received wherein a 14 year old male from Virginia (hereinafter VIC1) had been communicating through Instagram with a person utilizing Instagram account LEXIGURL1015. VIC1 had sent LEXIGURL1015 pornographic images of himself.

31. Detective Rosenbury interviewed VIC1 and his parents and determined that between the dates of 2/22/2019 and 2/23/2019, VIC1 engaged in online communications using Instagram and sent the LEXIGURL1015 account several images of himself that meet the definition of child pornography. VIC1 was under the impression that the person utilizing the LEXIGURL1015 account was a teenage female from California. VIC1 received from LEXIGURL1015 several pornographic images of an unknown female. Detective Rosenbury observed the activity on VIC1's cellular phone.

32. On 2/28/2019, Detective Rosenbury obtained a search warrant for Instagram account LEXIGURL1015 through the Fauquier Circuit Court in the State of Virginia. On 4/04/2019, Detective Rosenbury obtained the search warrant return and recovered all of the aforementioned messages and images sent between VIC1 and the person utilizing the LEXIGURL1015 account. The search warrant return also provided an email address of alexissmith1015@gmail.com for the subscriber and recent IP logs for the LEXIGURL1015

account. The account was registered on 2/17/2019 using IP address 98.5.196.189. The same IP address was used to login to the account during the time of the communications that occurred between VIC1 and the person using the LEXIGURL1015 account.

33. On 4/04/2019, pursuant to a subpoena issued by the Detective Rosenbury, Charter Communications reported that the subscriber of IP address 98.5.196.189 was Walter Gasiorek of 37 Lehigh Street, Buffalo, New York 14206. The subpoena return also provided a telephone number of (716)713-3052 and an email address of wgasiorek9601392@roadrunner.com.

34. On 4/10/2019 I conducted a utility check for the SUBJECT PREMISES with National Fuel who advised there was an active account at the SUBJECT PREMISES in the name of Walter Gasiorek. The account also listed a phone number of (716) 713-3052.

35. On April 11, 2019, I reviewed the search warrant return for the LEXIGURL1015 Instagram account. I confirmed all of the information provided by Detective Rosenbury. The following are excerpts of Instagram text messages between VIC1 and LEXIGURL1015:

*On 2/22/2019 @01:46:22 UTC, LEXIGURL1015 sent VIC1 an image of a teenage female and asked "what do u think of me?"*

*On 2/22/2019 @01:47:07 UTC, LEXIGURL1015 sent VIC1 a message stating, "send one back, I'll send another". In response, VIC1 sent LEXIGURL1015 an image of himself fully clothed.*

*On 2/22/2019 @02:05:57 UTC, LEXIGURL1015 sent VIC1 a message stating "send in just boxers, turn the flash off :p".*

*On 2/22/2019 @02:13:33 UTC, VIC1 sent LEXIGURL1015 a message stating, I just want to know what school do u go too". LEXIGURL1015 responded stating "mckinley in LA, u? VIC1 responded, "I go to Marshall middle in Va."*

*On 2/22/2019 @02:17:05 UTC, Vic1 then sends LEXIGURL1015 an image of his penis with a message stating "it's hairy". LEXIGURL1015 responded by sending a topless picture of a teenage female and with text message "send another;)". LEXIGURL1015 then tells VIC1, "do it from ur bed, sit down and put the cam below your dick chest and face;)." VIC1 then sends a message stating, "I'll send in a minute gotta make sure they think I'm sleeping". He then sends an image of his penis as directed by LEXIGURL1015. LEXXIGURL1015 sends VIC1 several more images of a naked female teenager.*

*On 2/22/2019 @02:38:13 UTC, LEXIGURL1015 sends VIC1 a message stating," take one with cum on your dick/chest;)." VIC1 then sends an image of his penis and his abdomen that has a clear substance on it.*

36. I examined the images that VIC1 sent of his face to LEXIGURL1015 and noted that he looks very young, well under the age of 18.

37. A further examination of the LEXIGURL1015 Instagram account found that there were several additional not yet identified minor males who had also sent LEXIGURL1015 images containing child pornography.

38. On April 11, 2019, I utilized a wireless internet detection device to determine the names and security status of any wireless networks operating in the vicinity of the

SUBJECT PREMISES. The results indicated several wireless networks, all of which were secured. On April 12, 2019, I again utilized a wireless internet detection device in the vicinity of the SUBJECT PREMISES and determined that there were several wireless networks available, all of which were secured.

39. On April 12, 2019, I conducted an open internet search of the SUBJECT PREMISES and learned that one of the resident's residing at the location is a substitute teacher and coach at a local middle school. I also spoke with a confidential source who confirmed this information.

40. Based on the forgoing, the above information indicates that on 2/22/2019, the pornographic files described herein were transmitted and traveled in interstate and foreign commerce via the Internet, and that those transmissions originated from an internet modem concealed inside the SUBJECT PREMISES.

### **III. SEARCHING COMPUTER SYSTEMS**

41. I have spoken with law enforcement personnel trained in computer evidence recovery who have knowledge about the operation of computer systems and the correct procedures for the seizure and analysis of computer systems.

42. These individuals have participated in the execution of numerous search warrants during which they have seized and/or examined computer systems. These individuals have also participated in several warrants that involved the search and/or seizure



of, and has been responsible for analyzing, seized electronic data and records from those systems.

43. Based on my experience and training, plus the common sense knowledge that in today's technological world computers, computer related media, and cellular telephones are used for communication and storage of data and information, it is reasonable to believe that some or all of the records sought to be seized will be in electronic/digital format.

44. Furthermore, based upon my training, experience, and consultations with law enforcement personnel who specialize in searching computer systems, I have learned that searching and seizing information from computer systems and other storage media (computers, PDAs, cellular telephones, MP3 Players, etc.) often requires agents to seize most or all the computer system or storage media to be searched later by a qualified computer forensic examiner in a laboratory or other controlled environment. This is true for the reasons set out below.

45. The volume of data stored on many computer systems and electronic storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. The hard drives commonly included in mere desktop computers are capable of storing millions of pages of text; the storage capacity of other electronic devices (e.g. a micro drive, a thumb drive, etc.) can also be significant. Unlike the search of documentary files, computers store data in "files" that cannot easily be reviewed. For instance, a single 1 gigabyte of storage media is the electronic equivalent of

approximately 500,000 pages of double spaced text. Most computer and electronic devices have capacities well in excess of a single gigabyte.

46. The search through the computer (or other electronic media) itself is a time consuming process. Software and individual files can be "password protected." Files can be placed in hidden directories; files can be mislabeled or be labeled with names that are misleading. Similarly, files that contain innocent appearing names ("Smith.ltr") can in fact be electronic commands to electronically cause the data to self destruct. Also, files can be "deleted," but, unlike documents that are destroyed, the information and data from "deleted" electronic files usually remains on the storage device until it is "over written" by the computer. For example, the computer's hard drive stores information in a series of "sectors," each of which contains a limited number of electronic bytes usually 512. These sectors are generally grouped to form clusters. There are thousands or millions of such clusters on a hard drive. A file's clusters might be scattered throughout the drive (for example, part of a memo could be at Cluster 163, while the next part of the memo might be stored at Cluster 2053). For a non-deleted file, there are "pointers" that guide the computer in piecing the clusters together. For a file that has been deleted, the "pointers" have been removed. Therefore, the forensic examination would include the piecing together of the associated clusters that made up the "deleted" file. Being aware of these pitfalls, the investigator/analyst must follow a potentially time consuming procedure to review the contents of the computer storage device so as to insure the integrity of the data and/or evidence. A single computer and related equipment could take many days to analyze properly.

47. Computer storage media are used to save copies of files and communications, and printers are used to make paper copies of these communications and files. Applications and associated data stored on the storage media are the means by which the computer can send, print and save such activity. Finally, password protected data and other security devices are often used to restrict access to or hide computer software, documentation or data. All these parts of a computer are integrated into the entire operation of a computer. In order to evaluate the evidence most effectively, the computers and all of the related computer equipment described above should be available to a computer investigator/analyst.

48. Therefore, based upon my knowledge, training, and experience, as well as information related to me by Special Agents and others involved in forensic examination of computers, I am aware that searches for and seizures of evidence from computers commonly require Agents to seize most or all of a computer system's input/output and peripheral devices (including other storage media), in order for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment. In order to fully retrieve data from a computer system, investigators must seize all the storage devices, as well as the central processing units (CPUs), and applicable keyboards and monitors which are an integral part of the processing unit.

49. Furthermore, searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is rarely possible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough

search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

50. The best practices for analysis of computer systems and storage media rely on rigorous procedures designed to maintain the integrity of the evidence and to recover hidden, mislabeled, deceptively named, erased, compressed, encrypted, or password protected data while reducing the likelihood of inadvertent or intentional loss or modification of data. A controlled environment, such as a law enforcement laboratory, is typically required to conduct such an analysis properly.

51. Therefore, it is respectfully requested that the warrant sought in the instant application authorize the search and seizure of all "computer hardware", "computer software" and related storage media, and other devices which may contain or assist in the retrieval of the records and documents described in Attachment B of this affidavit.

#### **IV. THE PLACE TO BE SEARCHED AND ITEMS TO BE SEIZED**

52. Based on the foregoing, there is probable cause to believe that at the SUBJECT PREMISES, which is more fully described and pictured in **Attachment A**, there is located evidence, fruits and/or instrumentalities of the violations specified in this affidavit.

53. Based on the foregoing, there is probable cause to believe that at the above location the items set out in **Attachment B** will be located, whether such items are stored in physical, documentary, or electronic form.

54. In addition it is and has been the standard and ordinary practice of FBI that during the execution of search warrants, Special Agents take entry and exit photographs of the premises to be searched, as well as photographs of the specific places in which items are found and from which items are seized. The purpose of this procedure is to preserve an accurate record of the condition and appearance of the premises upon the arrival and exit of the search team, and to preserve an accurate record of the locations within the premises where items are found and from which such items are seized.

## V. CONCLUSION

55. Based upon the above information, I believe that probable cause exists to believe there has been a violation of Title 18 U.S.C. Section 2251(a) [production of child pornography], Title 18 U.S.C. Section 2252A(a)(2) [receipt of child pornography] and 18 U.S.C. Section 2252A(a)(5)(B) [possession of child pornography] and that there is probable cause to believe that at **37 Lehigh Street, Buffalo, New York 14206**, which is more fully described and pictured in **Attachment A**, there is located those items set out in **Attachment B**.

56. In consideration of the foregoing, I respectfully request that this Court issue a search warrant for the premises known as **37 Lehigh Street, Buffalo, New York 14206**,

which is more fully described and pictured in **Attachment A**, authorizing the search of the aforementioned premises for the items described in **Attachment B**.

57. Finally, it is respectfully requested that this Court issue an Order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the required inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the premises to be searched).



Michael Hockwater, Task Force Officer  
Federal Bureau of Investigation

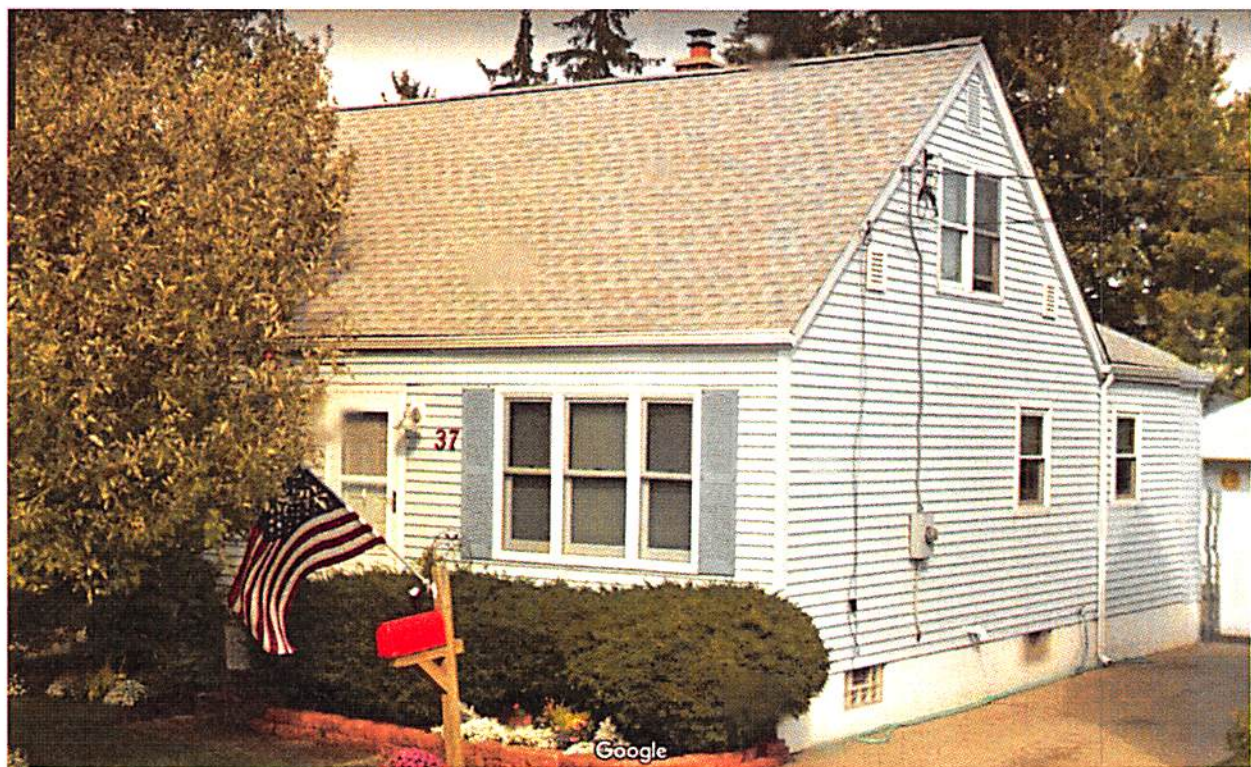
Sworn and subscribed to before me  
this 15<sup>th</sup> day of April 2019.



United States Magistrate Judge Jeremiah J. McCarthy

**ATTACHMENT A**  
**Premises to be Searched**

**37 Lehigh Street, Buffalo, New York 14206**, is a 1 ½ story cape cod style single-family residence on the east side of the street. It has blue siding and white trim. The number “37” is displayed on the front of the house next to the front door. A photograph of the residence is included below.





**ATTACHMENT B**  
**The Items to be Searched**

The items to be searched for and seized at the location listed in Attachment A, whether in physical, documentary, or electronic form, that pertain to violations of Title 18, United States Code, 2251(a) [production of child pornography], Title 18 U.S.C. Section 2252A(a)(2) [receipt of child pornography] and 18 U.S.C. Section 2252A(a)(5)(B) [possession of child pornography], are as follows:

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, and any mechanism used for the production, receipt, distribution, advertisement, or storage of the same, including but not limited to:

Any computer, computer system and related peripherals including any data processing devices and software (including but not limited to central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, computer compact disks, CD-ROMS, DVD, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, camcorders, and related communications devices such as cables and connections); related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices and electronic tone-generating devices); cellular telephones; as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

2. Any and all computer passwords, counter-forensic programs, and other data security devices designed to restrict access to, hide, or destroy computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

3. Any and all documents, records, images, videos, emails, email software, associated email addresses, email address book contents, internet history, browsing history, internet search history, cookies, deleted files, bookmarked and favorite web pages, user typed web addresses, desktop shortcuts, path and file names for files opened through any media and/or image viewing software, chat software, chat files, chat logs, chat names used, peer to peer software, peer to peer files, newsgroup postings by the user, IP addresses assigned, and other evidence pertaining to the production, receipt, and possession of child pornography, sex trafficking of minors, and/or the coercion and enticement of minors for illegal sexual activity;



4. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence.

5. Documents and records regarding the ownership, usage and/or possession of the searched premises.

6. Photographs: Entry and exit photographs of the premises to be searched, as well as photographs of the specific places in which items are found and from which items are seized.